

Khalda Petroleum Company		Petrofac 	
Project: Salam Gas Trains (SGT3 & 4) Project			
Location: Egypt			
Purchase Order No.:	187030017	Petrofac Project No.:	J1-187

DOCUMENT TITLE	SAFETY INTEGRITY LEVELS (SIL) ANALYSIS		
P.O DESCRIPTION	HIGH INTEGRITY PRESSURE PROTECTION SYSTEM (HIPPS)		
EQPT. TAG No.	EIN01	CONTRACT No.	1820
Vendor Document No.	200177AT_SIL_00002_Rev.B	RED CODE	G14
☒ A	WORK MAY PROCEED. NO MORE SUBMISSION FOR REVIEW IS REQUIRED.		
☐ B	REVISE AND RESUBMIT. WORK MAY PROCEED SUBJECT TO INCORPORATION OF THE CHANGES INDICATED.		
☐ C	REVISE AND RESUBMIT. WORK MAY NOT PROCEED.		
☐ D	FOR INFORMATION/ REFERENCE. REVIEW NOT REQUIRED. WORK MAY PROCEED.		
Reviewing Engineer's Name (IN BLOCK LETTERS), Sign and Date			
Name: HIMANSHU SARSENA		Sign: 	Date: 12/9/07

PETROFAC INTERNATIONAL LTD.					
DOCUMENT NO.:					
JOB No.	PO No.	Tag No.	Code No.	Serial No.	REV.
J1	187	030017	EIN01	G14	001 B

CCI VALVE TECHNOLOGY VIENNA	
Doc. No.	187030017-EIN01-G14-001
Revision	B
Date	2007-09-06
File Ref.	200177AT_SIL_00002

PETROFAC E & C INT'L LTD.	
Job No.: J1 - 187	
☒ A. Work may proceed, No more submission for review is required. ☐ B. Revise and resubmit. Work may proceed subject to incorporation of changes indicated. ☐ C. Revise and resubmit. Work may not proceed. ☐ D. Review not required. Work may proceed.	
Signed: 	
Permission to proceed does not release fabricator of the obligation to furnish the equipment in accordance with purchase order drawings, specification, applicable code and does not constitute acceptance or approval of fabricator's design.	
By: HS	Date: 12/9/07



Revision history

Rev	Date	Description of Change
A	30.07.2007	First Issue
B	06.09.2007	Revised for Approval

Approval Authority: (Project Manager / Project Engineering Manager)

Owner	Developer	Reviewer	Approver
-	ILR	KAL	MIG

Summary / Holds

Sr.	Description	Page
1.	Safety Integrity Level (SIL) Analysis (SIL ANALYSIS REPORT)	26



SIL ANALYSIS REPORT

HIPPS - COMPLETE LOOP

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG N°	200177AT_SIL_00002
			FILE	
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N° 1	OF N° 29

1. General

1.1 Introduction

The objective of this document is to classify the Safety Integrity Level (SIL) of the Safety Critical Loops for the **HIPPS** Project. The SIL values are used to define the reliability requirements for safety dedicated instrument and control equipment. All the components that lead to Safety Loop have been considered for this analysis.

IEC61508 provides the guideline to design and to verify electrical, electronic and or programmable electronic systems that are used to perform safety functions. This document provides SIL classification method using IEC61508 standard as the reference documentation.

SIL classification is carried out for Local Safety Functions of the HIPPS.

1.2 Abbreviations

Here below a list of abbreviations used in this document with the relevant meaning:

FIT = Failures In Time ($1 \times 10^{-9}/h$)

FMEA = Failure Mode Effect Analysis

FMECA = Failure Mode Effect & Criticality Analysis

FMEDA = Failure Mode Effect & Diagnostic Analysis

HFT = Hardware Fault Tolerance

MTBF = Mean Time Between Failures

MTTF = Mean Time To Failures

MTTR = Mean Time To Repair

PES = Programmable Electronic System

PFD = Probability of Failure on Demand

PFH = Probability of Failure per Hour

PST = Partial Stroke Test

SFF = Safe Failure Fraction (%)

SIF = Safety Instrumented Function

SIL = Safety Integrity Level

SIS = Safety Instrumented System

T1 = Proof Test Interval

λ = Total failure rate (1/h)

λ_d = Failure Rate, dangerous (1/h)

λ_s = Failure Rate, safe (1/h)

λ_{dd} = Failure Rate, dangerous detectable (1/h)

λ_{du} = Failure Rate, dangerous undetectable (1/h)

λ_{sd} = Failure Rate, safe detectable (1/h)

λ_{su} = Failure Rate, safe undetectable (1/h)

λ^L = Failure Rate, fails low (1/h)

λ^H = Failure Rate, fails high (1/h)

β = Common Cause Failure Fraction (%)

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
SHEET N° 2			OF N° 29	

2. Safety Integrity Level (SIL)

Safety Integrity Level is the discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety function, where SIL 4 has the highest ranking of safety integrity and SIL 1 has the lowest. The SIL level required is a function of the effect and frequency of a control system failing to respond to a demand, leading to hazardous or undesirable consequences.

2.1 Applicable Documents

2.1.1 Reference Codes and Standards

IEC61508 1-7, the international standard on Functional Safety of electrical / electric / programmable electronic safety-related systems;
IEC61511 1-3, the international standard on Safety Instrumented Systems for the Process Industry.

2.1.2 Project Documentation

The followings documents have been used for SIL Classification purposes:

- Functional Design Specification (doc. N° 200177AT_CCD_00004)
- HIPPS System Architecture (doc. N° 200177AT_CCD_00008)
- Astava Manifold Double Block & Bleed reliability parameters (attached)
- ABB Pressure Transmitter 2600T reliability parameters (attached)
- Honeywell Pressure Transmitter ST3000 reliability parameters (attached)
- Rosemount Pressure Transmitter 3051S_C reliability parameters (attached)
- Asco Solenoid Valve 327 reliability parameters (attached)
- Rotork Pneumatic Actuator GP reliability parameters (attached)
- Rona Ball Valve reliability parameters (attached)

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
SHEET N°	3		OF N°	29

2.2 General

The loop, which generate possible hazardous scenario consequences due to failure on demand, has been classified according to the IEC 61508 standard with the use of the attached SIL Classification Sheets (Table 1).

2.3 SIL Reliability Targets

Table 1 provides the recommended target reliability for each SIL as based on IEC 61508 part-1 7.6.2.9.

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Average probability of failure to perform its design function on demand)	HIGH DEMAND OR CONTINUAL MODE OF OPERATION (Probability of a dangerous failure per hour)
4	$>10^{-5}$ to $<10^{-4}$	$>10^{-9}$ to $<10^{-8}$
3	$>10^{-4}$ to $<10^{-3}$	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-3}$ to $<10^{-2}$	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-2}$ to $<10^{-1}$	$>10^{-6}$ to $<10^{-5}$

Table 1 - Probability of Failure on Demand according to the operation mode

3. SIL verification

The scope of this phase is to calculate the probability of failure on demand (PFDavg) for **HIPPS** control loop. The PFD analysis has been performed for sensors, logic solvers and final elements. The first step was the creation of the reliability block diagrams (RBD) for the complete loop. The RBD consists of three sub-blocks:

1. sensors (Interlocking Manifold, Pressure Transmitter, Ex-I Isolator)
2. logic solver (Input, CPU, Connector, Output)
3. Final elements (Solenoid, Actuator, Valve)

The average PFD was calculated for every sub blocks according to the equations in the IEC61508. Architectural constraints were applied in order to identify the maximum hardware safety integrity that can be claimed for the equipment under analysis. PFD and architectural constraints allow to estimate the SIL (safety integrity level).

Failure common causes factor has been chosen to be conservatively 5% for sensors and 10% for final elements.

With respect to this analysis the HIPPS loop considered has been evaluated supposing a low demand mode of operation. Therefore, in Table 1 the first two columns have been taken into account only.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 4	OF N° 29

3.1 Reliability Data

Reliability parameters used for the SIL analysis have been taken from the documentation supplied by the manufacturers of components. In particular, for the logic solver has been used the SIL calculation tool supplied by the logic solver manufacturer (Hima), where the reliability parameters of their components are included.

4. Hardware fault tolerance

Final elements are classified as type A devices and the minimum hardware fault tolerance level has been verified according to table 2. Sensors and logic solver are classified as type B devices and the minimum hardware fault tolerance level has been verified according to table 3.

Safe Failure Fraction SFF	Hardware Fault Tolerance (see note 1)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Note 1 : A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

Table 2 - Architectural constraints on type A safety related sub-systems

Safe Failure Fraction SFF	Hardware Fault Tolerance (see note 1)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Note 1 : A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

Table 3 - Architectural constraints on type B safety related sub-systems

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 5	OF N° 29

5. SIL calculation report (from SILence calculation tool)

4796ABA3

Contents

Contents

1 System configuration:200177AT - H51q-HRS - rev-A	
1.1 File History	
1.1.1 Change dated 25.07.2007 - 19:58:09	
1.2 System configuration:	
1.2.1 Libraries	
1.3 Result for T1 ≈2 years	
1.3.1 Lo-Demand-Result	

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 6	OF N° 29

1 System configuration:200177AT - H51q-HRS - rev-A

File: C:/Documents and Settings/ts_toscana/Desktop/200177AT - H51q-HRS - rev-A.ssy
 File-CRC: 4796aba3

1.1 File History**1.1.1 Change dated 25.07.2007 - 19:58:09**

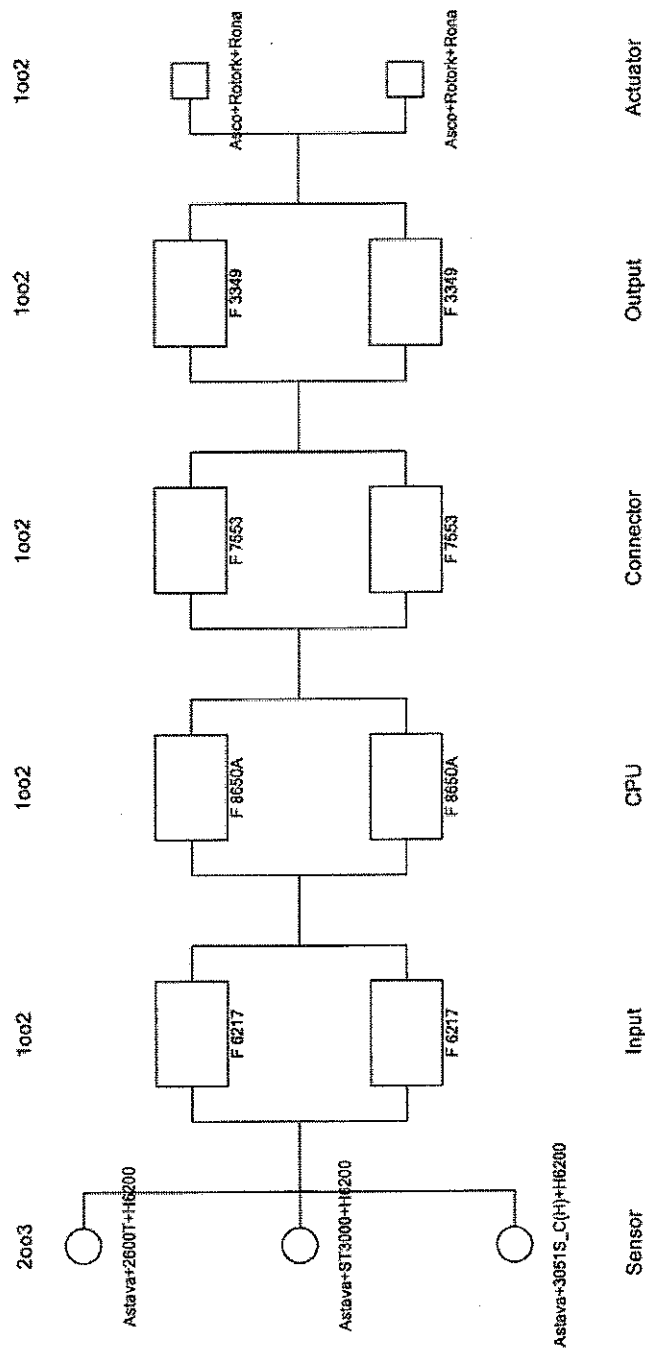
Version: Rev-A
 Author: Leonardo Fusi
 Comment: The total HIPPS Proof Test interval time is 2 years.
 Final Elements PFD's are based on Partial Stroke Test interval time of 1 month.
 Partial Stroke Test have a 60% diagnostic coverage of dangerous failures relevant to the final elements.
 Each Sensor module is including the series of the manifold line, the pressure transmitter and the Ex-i isolator.
 Each Actuator module is including the series of the solenoid valve, the actuator with its quick exhaust devices and the valve.
 Common Cause Failures (Beta) is 5% for the sensors and 10% for final elements.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 7	OF N° 29

1.2 System configuration:

4796ABA3

1.2 System configuration:



B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			FILE NO	200177AT SIL_00002
			DWG NO	
			FILE	
			SHEET N°	8 OF N° 29

SIL ANALYSIS REPORT

This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request

4796ABA3

1.2.1 Libraries

Sensor: Architecture2003

Astava+2600T+H6200 (ID: 69981E3E-488D2B5B) Manifold DB&B + PT 2600T + Hima Ex-I Isolator
 Astava+ST3000+H6200 (ID: 9E0B3E1D-DF8B6F6) Manifold DB&B + PT ST3000 + Hima Ex-I Isolator
 Astava+3051S_C(H)+H6200 (ID: F333988F-ABC2780A) Manifold DB&B + PT 3051S_C + Hima Ex-I Isolator

Input: Architecture1002

F 6217 (ID: 89D0E67A-483AC69C) 8-channel analogue input module
 F 6217 (ID: 89D0E67A-483AC69C) 8-channel analogue input module

CPU: Architecture1002

F 8650A (ID: 89D0E67A-5B7CDB53) Central module
 F 8650A (ID: 89D0E67A-5B7CDB53) Central module

Connector: Architecture1002

F 7553 (ID: 89D0E67A-B76DADA8) Coupling module
 F 7553 (ID: 89D0E67A-B76DADA8) Coupling module

Output: Architecture1002

F 3349 (ID: 89D0E67A-866CDCE0) 8-channel digital output module
 F 3349 (ID: 89D0E67A-866CDCE0) 8-channel digital output module

Actuator: Architecture1002

Asco+Rotork+Rona (ID: A89A85EA-3647FF5B) Solenoid + Actuator + Valve (PST=1/24TI)
 Asco+Rotork+Rona (ID: A89A85EA-3647FF5B) Solenoid + Actuator + Valve (PST=1/24TI)

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems[®] CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request		
		FILE	200177AT_SIL_00002	
		DWG No		
		SHEET N°	9	OF N° 29

4796ABA3

1.3 Result for T1 =2 years

1.3.1 Lo-Demand-Result

System / Module	HIMA-Lib.	SIL	PED	SEF	MTTF	Percent of PFx
Total result		3	4.353e-004	99.36%	0.63y	100.00%
Sensor		4	7.945e-005	93.18%	19.21y	18.25%
Astava+2600T+H6200		4	6.069e-005	93.75%	56.19y	13.94%
Astava+ST3000+H6200		4	6.208e-005	91.43%	75.18y	14.26%
Astava+3051S_C(H)+H6200		4	7.945e-005	93.18%	47.73y	18.25%
Input		4	1.873e-007	99.84%	51.58y	0.04%
F 6217		4	1.873e-007	99.84%	103.17y	0.04%
F 6217		4	1.873e-007	99.84%	103.17y	0.04%
CPU		4	5.821e-007	99.78%	29.68y	0.13%
F 8650A		4	5.821e-007	99.78%	59.35y	0.13%
F 8650A		4	5.821e-007	99.78%	59.35y	0.13%
Connector		4	5.791e-008	99.95%	102.00y	0.01%
F 7553		4	5.791e-008	99.95%	203.99y	0.01%
F 7553		4	5.791e-008	99.95%	203.99y	0.01%
Output		4	3.294e-007	99.76%	24.76y	0.08%
F 3349		4	3.294e-007	99.76%	49.51y	0.08%
F 3349		4	3.294e-007	99.76%	49.51y	0.08%
Actuator		3	3.547e-004	99.52%	0.70y	81.48%
Asco+Rotork+Rona		3	3.547e-004	99.52%	1.41y	81.48%
Asco+Rotork+Rona		3	3.547e-004	99.52%	1.41y	81.48%

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request		
		FILE DWG No 200177AT_SIL_00002		
		SHEET N° 10 OF N° 29		

6. Final SIL Calculation result for the entire HIPPS

PFD_{sys} : 4.353x10⁻⁴ (SIL 3)
 Architectural Constraints : SIL 3

Proof Test interval time (T1) : 2 years
 Partial Stroke Test interval time : 1 month

COMPONENTS FAILURES RATES:

System / Module	λ_{du}	λ_{dd}	λ_s	PFD _{avg} (T1=2 years)	Note
ABB 2600T Sensor module (1)	1.2706e-07	1.0452e-06	8.5924e-07	7.945e-05	Sensor subsystem 2oo3
Honeywell ST3000 Sensor module (1)	1.3006e-07	7.532e-07	6.3524e-07		
Rosemount 3051S_C Sensor module (1)	1.6306e-07	1.1532e-06	1.07524e-06		
Hima F6217 Logic Solver Input modules	9.5938e-10	2.3698e-07	3.5546e-07	1.873e-07	Logic Solver subsystem 1oo2
Hima F8650A Logic Solver CPU modules	3.0120e-09	6.5589e-07	7.4050e-07	5.821e-07	
Hima F7553 Logic Solver Connector modules	2.2674e-10	2.2651e-07	2.5026e-07	5.791e-08	
Hima F3349 Logic Solver Output modules	1.7451e-09	2.8675e-07	4.2961e-07	3.294e-07	
Asco + Rotork + Rona Ball Valve Actuator module	9.127e-07	0	8.0217e-05	3.547e-04 (PST=1 month)	Actuator subsystem 1oo2

(1) Including interlocking manifold Astava DB&B and the Hima Ex-i isolator H6200

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N° 11	OF N° 29

7. Attached Documentation: Reliability Data of field devices and logic solver

(on the following pages)

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT 		

7.1 Astava Interlocking Manifold

Certificate

The Certification Body RWTÜV Systems GmbH of Product Safety and Medical Devices hereby certify

ASTAVA B.V.
Industrieweg 30
7944 HS Meppel, Netherlands

that the product

**Interlocking Manifold, Types 1002, 2003, 1004
with Block-Bleed or Block-Bleed-Block Function**

meets the below mentioned requirements:

- IEC 61508:2000; SIL 4; Functional safety of electrical/electronic/programmable electronic safety-related systems

Based on the report No. 701-004/2004T in the valid version

This certificate entitles the holder to use the mark



Certificate Register No. SAS-2063/04
File reference: 2.4-4243/04
Valid to: 2009-08-18

Essen, 2004-08-18

Michael Eck

Dr. Ulrich Adolph

04

RWTÜV Systems GmbH
Postfach 10 32 61 - 45032 Essen

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			200177AT_SIL_00002	
			№ DWG	
			FILE	
SIL ANALYSIS REPORT			SHEET N° 13	OF N° 29
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request				

8.2.5 Modelling of the maintenance services

In the maintenance services the system is tested at regular, extended intervals to ascertain any (previously undetected) faults. During services the whole system is out of operation. during the service all faults are detected. The repair of undetected faults is conducted within a certain period at Astava. After the repair at Astava, the repaired interlocking manifold is installed on site.

A graphic presentation of the condition transitions modelled is given in Chap. 11.1 Annex A (Figure 8)

Figure 8 shows graphically the whole model, including maintenance phases and common cause.

8.2.6 Calculations

Starting with the data of Astava for performance in practice, the corresponding lamda values were determined (see Chap. 8.1.4). the common cause was assumed as being 2% .

The calculation is therefore based on the following coefficients of the transition rates, taking account of a common cause factor of $\beta=2\%$. The index c here stands for failure due to common cause faults.

Table 5: Table of transition rates for the whole system

Transition rates in fit	Whole system
$\lambda_{DUN} = (1 - \beta) \lambda_{DU}$	84.9
$\lambda_{DUC} = \beta \cdot \lambda_{DU}$	1.8
Proof-check (maintenance) interval μ_T	1/4380 h ⁻¹
Repair time μ_B	1/720 h ⁻¹
Installation μ	1/8 h ⁻¹
Usability time of the system	30 years = 262800 h

The factors of the respective transitions are obtained in accordance with Table 6.

File: SAS.TB.Gearbox.signed.v1.02.doc
Test Report No. 1.02
Date: 2004-07-28
Page 28 of 37

Safety Approval Service – SAS

RWTÜV Systems GmbH
Hübnersstr. 3
D-86150 Augsburg

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG №	200177AT_SIL_00002
			FILE	
SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N°	14 OF N° 29

7.2 ABB Pressure Transmitter 2600T

CERTIFICATE • CERTIFICADO • CERTIFICAT • CERTIFIKAT

CERTIFICATE

No. Z10 04 02 42206 007



Holder of Certificate: ABB SACE S.p.A.
Via Statale 113
I - 22016 Lenno (Co)
Italy

Factory(ies): 42206

Certification Mark:



Product: Safety Related Programmable Electronic System

Model(s): SAFETY 2600T PRESSURE TRANSMITTERS

Parameters:

Structure - Safety Integrity Level:	1oo1 - SIL2
Pressure range:	0 to 30000 kPa
Nominal current range:	4 to 20 mA
Transmitter failure mode:	<3.7 or >22 mA
Compliance voltage:	10.5 to 42 Vdc
Operating temperature range:	-40° C to +85° C

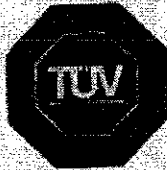
Tested according to:

• IEC 61508:1998, 2000 / SIL2	• EN 61000-4*:1993, 1996
• IEC 60068-2*:1974, 1990	• EN 55011:1988
• IEC 529:1989	• EN 55022:1988

The listed product was tested on a voluntary basis and complies with the essential requirements.
The certification mark shown above can be affixed on the product. See also notes overleaf.

Test report No. AL63021C, E-(Z10 02 08 42206 005)

Date: 2004-02-20



TUV PRODUCT SERVICE GMBH • Zertifizierungsstelle • Ridlerstrasse 65 • D-80333 München
Gruppe TÜV Süddeutschland

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	NO	200177AT_SIL_00002
			DWG NO	
		This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	FILE	
			SHEET N°	15 OF N° 29

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the 'Safety Related Field Device' SAFETY 2600T PRESSURE TRANSMITTER comply with the testing criteria specified in clause 3 for intermittent or continuous mode of operation in applications up to SIL 2.

The safe state < 4 mA or > 20 mA of the analog output is user configurable.

General conditions and restrictions for application, commissioning, run-time are defined in clause 5.

4.1.1 'Safe Failure Fraction' and quantitative analysis of the hardware

The Diagnostic Coverage and Safe Failure Fraction evaluation has been elaborated following the requirements of IEC 61508 part 2 and 6. For the calculation of the failure rate λ , the software „Reliability Workbench by ITEM Software Ltd“, based on MIL 217 Handbook, has been used. The total results are listed in table 4.

Safe failure	295 FIT
Dangerous failure	706 FIT
Safe detected failure	134 FIT
Safe undetected failure	160 FIT
Dangerous detected failure	669 FIT
Dangerous undetected failure	37 FIT
Do not care	181 FIT
Diagnostic Coverage	94,88 %
Safe Failure Fraction	96,73 %

Table 4: Result of the FMEA

The 'Proof Test Interval' (see below) may be specified by using the method of calculation of the IQSE (in accordance with the QSAA statistical calculation), within the assemblies have to be completely tested in order to detect an initial fault before combination with a possible second fault becomes harmful. Most of the following abbreviations can be found in the international norm IEC 61508-6.

TÜV Automotive GmbH
Automation, Software and Electronics - IQSE
Ridlerstr. 65
D-80339 München
Phone: +49 (89) 5791-4617; Fax: -4438

Report No.: AL63021C, Revision 1.3
Order No: 70029198
Mr. Henke, Mr. Blum
2004-02-20
Page 8 of 15

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems™ CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG No	200177AT SIL 00002
			FILE	
SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N°	16 OF N° 29

7.3 Honeywell Pressure Transmitter ST3000

TUV NORD

Certificate

Honeywell International Inc.
Industrial Measurement & Control
1100 Virginia Dr.
Fort Washington, PA 19034, USA

The safety related ST3000 Pressure Transmitter

meets the requirements listed in the following standard

IEC 61508-1:1998, IEC 61508-2:2000, IEC 61508-3:1999, Functional safety of
electrical/electronic/programmable electronic safety-related systems
SIL 2 capability for single transmitter use
SIL 3 capability for multiple transmitter use

based on report no. SAS-128/2006T in the valid version
This certificate entitles the holder to use the certification mark



Certificate Register No. SAS-139/06, Vers. 1.0, Augsburg, 2006-Dec-12

File reference: 24-115/06

Valid to: 2011-Dec-12

TUV NORD System GmbH & Co. KG
Branch South
Helmstr. 27
86450 Augsburg / Germany

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG No	200177AT_SIL_00002
			FILE	
SIL ANALYSIS REPORT			SHEET N° 17	OF N° 29
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request				



Management summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the ST3000 pressure transmitter. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the ST3000 pressure transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The ST3000 pressure transmitter is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. All other possible output variants are not covered by this report. The device can be equipped with or without display.

The ST3000 pressure transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the device has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 2 as a single device.

The failure rates for the ST3000 pressure transmitter are listed in Table 1.

Table 1 Failure rates ST3000 pressure transmitter

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	377
Fail Detected (detected by internal diagnostics)	268
Fail High (detected by the logic solver)	20
Fail Low (detected by the logic solver)	89
Fail Dangerous Undetected	40
No Effect	64
Annunciation Undetected	6

Table 2 lists the failure rates for the ST3000 pressure transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents. It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected according to IEC 61508 (worst-case assumption).

Table 2 Failure rates and SFF according to IEC 61508

Device	λ_{ed}	λ_{su}^2	λ_{dd}	λ_{du}	SFF
ST3000 pressure transmitter	0 FIT	70 FIT	377 FIT	40 FIT	91.8%

These failure rates are valid for the useful lifetime of the product, see Appendix A: Lifetime of critical components.

¹ Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

² It is important to realize that the "no effect" failures are included in the "safe undetected" failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	200177AT_SIL_00002	
			DWG N°	
			FILE	
		This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	SHEET N° 18	OF N° 29

7.4 Rosemount Pressure Transmitter 3051S_C

Certificate

The Certification Body RWTÜV Systems GmbH of Product Safety and Medical Devices hereby certify

Rosemount Inc.

8200 Market Blvd.
Chanhassen, MN 55317 USA

that the product

**3051S SIS Pressure Transmitter
with Safety Feature Board**

meets the below mentioned requirement

IEC 61508: 2000; Part 1 to Part 7
Functional safety of electrical/electronic/programmable
electronic safety-related systems;
Low Demand; Type B;
SIL 2 capability for hardware (single transmitter use)
SIL 3 capability for software (multiple transmitter use)

based on the report No. 701-070/2002T in the valid version.

This certificate entitles the holder to use the mark:



Certificate Register-No.: SAS0558/04
File reference: 2.4-4055/04
Valid to: 2009-03-14

Essen, 2004-03-15

Michael Eck

Dr. Ulrich Adolph

04

RWTÜV Systems GmbH
Postfach 10 32 61 - 45032 Essen

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			200177AT_SIL_00002	
SIL ANALYSIS REPORT				
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N° 19	OF N° 29

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 3051S SIS Pressure Transmitter. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the 3051S SIS Pressure Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 3051S SIS Pressure Transmitter is a two-wire, 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. All other possible output variants are not covered by this report. The different devices can be equipped with or without display.

Table 1 gives an overview of the different versions that belong to the considered 3051S SIS Pressure Transmitter.

Table 1: Version overview

3051S_T In-Line	3051 S In-Line Pressure Transmitter
3051S_C Coplanar	3051S Coplanar Pressure Transmitter

The 3051S SIS Pressure Transmitter is classified as a Type B¹ device according to IEC61508, having a hardware fault tolerance of 0. The analysis shows that the device has a Safe Failure Fraction between 90 and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 2 as a single device.

The failure rates for the 3051S_T In-Line Pressure Transmitter are as follows:

$$\lambda^H = 59 \cdot 10^{-9} \text{ failures per hour}$$

$$\lambda^L = 750 \cdot 10^{-9} \text{ failures per hour}$$

$$\lambda^{DU} = 88 \cdot 10^{-9} \text{ failures per hour}$$

Table 2 lists the failure rates for 3051S_T In-Line Pressure Transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 2: Failure rates according to IEC 61508 - 3051S_T In-Line

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
Low trip	750 FIT	468 FIT	59 FIT	68 FIT	94.9%
High trip	59 FIT	468 FIT	750 FIT	68 FIT	94.9%

(Note that the SU category includes failures that do not cause a spurious trip)

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

© exida.com L.L.C.

William M. Goble – John C. Grebe

ros 02-11-07 r001 v230.doc, 12/17/2004

Page 2 of 20

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
	A	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG N°	200177AT_SIL_00002
			FILE	
SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N°	20 OF N° 29

The failure rates for the 3051S_C Coplanar Pressure Transmitter are as follows:

$$\lambda^H = 62 * 10^{-9} \text{ failures per hour}$$

$$\lambda^L = 777 * 10^{-9} \text{ failures per hour}$$

$$\lambda^{DU} = 73 * 10^{-9} \text{ failures per hour}$$

Table 2 lists the failure rates for 3051S_C Coplanar Pressure Transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 3: Failure rates according to IEC 61508 - 3051S_C Coplanar

Failure Categories	λ_{sd}	λ_{su}	λ_{ds}	λ_{du}	SFF
Low trip	777 FIT	448 FIT	62 FIT	73 FIT	94.6%
High trip	66 FIT	448 FIT	777 FIT	73 FIT	94.6%

(Note that the SU category includes failures that do not cause a spurious trip)

These failure rates are valid for the useful lifetime of the product, which is > 50 years.

A user of the 3051S SIS Pressure Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.5 along with all assumptions.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 SIL ANALYSIS REPORT			200177AT_SIL_00002	
 CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 21	OF N° 29

7.5 Hima Logic Solver H51q-HRS (SIL 3 certified)



TÜV Rheinland Group

TÜV Industrie Service GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT CERTIFICATE

Nr./No. 968/EZ 129.06/05

Prüfgegenstand Product tested	Safety Related Programmable Electronic System	Hersteller Manufacturer	HIMA Paul Hildebrandt GmbH + Co. KG Albert-Bassermann-Straße 28 D-68782 Brühl bei Mannheim
Typbezeichnung Type designation	H41q-MS, H41q-HS, H41q-HRS H51q-MS, H51q-HS, H51q-HRS	Verwendungszweck intended application	Safety Related Programmable Electronic System for process control, Burner Management (BMS), emergency shut down, machinery, where the safe state is the de-energized state. Fire and Gas, where the safe/demand state is the de-energized or energized state.
Prüfgrundlagen Codes and standards forming the basis of testing	IEC 61508, Part 1-7:2000 IEC 61511:2004 EN 954-1:1996 DIN VDE 0118:1989, EN 50156-1:2004 EN 12067-2:2004, EN 298:2003, EN 230:1990 NFPA 85:2001 EN 61131-2:2003 EN 61000-6-2:2001, EN 61000-6-4:2001 EN 54-2:1997, NFPA 72:2002		
Prüfungsergebnis Test results	The system is suitable for safety related applications up to SIL 3 (IEC 61508, IEC 61511) and CAT 4 (EN 954-1).		
Besondere Bedingungen Specific requirements	For the use of the systems, the Safety Manual, the User Manual and the actual revision of the official list of product documentation, hardware modules and software components released by HIMA and TÜV Rheinland have to be considered.		



Der Prüfbericht-Nr.: 968/EZ 129.06/05 vom 2005-08-02 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no.: 968/EZ 129.06/05 dated 2005-08-02 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products, which are identical with the product tested.

TÜV Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Gahlen Stein, 51105 Köln
Postfach 91 00 51, 51101 Köln

H. Gall

2005-08-02

Datum/Date

Firmenstempel/Company seal

Unterschrift/Signature

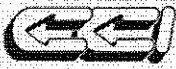
B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
We Solve Control Valve Problems[®] CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request		
			DWG N°	200177AT_SIL_00002
			FILE	
			SHEET N°	22
			OF N°	29

NTTR	8 Stunden	SIL-zertifizierte Baugruppe nach IEC 61508	MTTF in Jahren	$\lambda_{0_INTT} / h^{-1}$	λ_S / h^{-1}	λ_{OP} / h^{-1}	λ_{QU} / h^{-1}	$PFD_{DECERR} / 1$ ($T_1 = 10$ Jahre)	PFH_{DECERR} / h^{-1} ($T_1 = 10$ Jahre)	SFF	SIL	HFT
		H 6200	51.41	2.220450E-06	5.662400E-07	3.761938E-07	3.361080E-09	6.755535E-05	3.467408E-09	99.6443%	3	0

HiQuad		SIL-zertifizierte Baugruppe nach IEC 61508	MTTF in Jahren	$\lambda_{0_INTT} / h^{-1}$	λ_S / h^{-1}	λ_{OP} / h^{-1}	λ_{QU} / h^{-1}	$PFD_{DECERR} / 1$ ($T_1 = 3$ Jahre)	PFH_{DECERR} / h^{-1} ($T_1 = 3$ Jahre)	$PFD_{DECERR} / 1$ ($T_1 = 10$ Jahre)	PFH_{DECERR} / h^{-1} ($T_1 = 10$ Jahre)	SFF	SIL
		F 3349	49.51	2.305600E-06	4.296100E-07	2.857450E-07	1.745060E-09	7.591288E-06	1.760327E-09	2.230632E-05	1.766173E-09	99.7670%	3
		F 6217	103.17	1.105500E-06	3.554900E-07	2.368400E-07	9.593800E-10	9.732448E-06	9.632087E-10	2.864697E-05	9.639427E-10	99.8389%	3
		F 7553	203.99	5.586000E-07	2.502300E-07	2.285133E-07	2.267400E-10	3.986438E-05	6.764891E-10	9.777478E-06	5.755791E-10	99.9525%	3
		F 8550A	59.35	1.923400E-06	7.405000E-07	6.538800E-07	3.017040E-09	1.070004E-05	3.676895E-09	2.897644E-05	3.651869E-09	99.7849%	3



The safe decision.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh. 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG No	200177AT SIL_00002
			FILE	
			SHEET N°	23
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			OF N°	29

SIL ANALYSIS REPORT

7.6 Asco Solenoid Valve 327 series



Certificate

Manufacturer: ASCO Controls BV
 Industrielaan 21
 3925 BD Scherpenzeel
 Nederlande

Product: 3/2 Way Valves
Type: ...327 ...

Intended Use: Automatic Solenoid Valve
 with safety function

Test results: The valves of the above mentioned type series
 are suitable for use in safety related systems
 with Hardware Fault Tolerance of 1 or 2 up to and
 including SIL 4 according to IEC 61508
 Detailed test results can be drawn from report
 No. S 194/02 dated 18.02.2003.

The suitability for certain fields of application can
 only be assessed by additional evaluation of
 further components of the subsystem.

This certificate remains valid until February 2008.

Cologne, February 18, 2003

Test laboratory for energy
 appliances
 Head of Laboratory

 Dipl.-Ing. F. Rick

Group TÜV Rheinland/Berlin-Brandenburg
 TÜV Instandhaltung und Energiesysteme GmbH, Am Grauen Stein, D-51105 Köln

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.	
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.	
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.	
 We Solve Control Valve Problems™ CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT		DWG No	200177AT SIL 00002
				FILE	
				This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	

ASCO JOUCOMATIC S.p.A.
Via Zambelletti 8/10
20021 BARANZATE DI BOLLATE (MI)
Tel. 02.35693.1
Fax 02.35693300
e-mail: aji@ascojoucomatic.it

SIL reliability data Asco Joucomatic 327 & 551 series

1. Lambda SD	= 0
2. Lambda SU	= 800×10^{-7}
3. Lambda DD	= 0
4. Lambda DU	= 8×10^{-7}
5. MTTR	= < 0,5h
6. Type	= "A"
7. Hard fault tolerance	= 1 o 2
8. Confidence level	= 95%
9. SFF	= 0,99

Note: "Off line proof Test interval" T_i = 1 year

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien			DWG N°	200177AT_SIL_00002
			FILE	
			SHEET N°	25 OF N° 29
SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request				

7.7 Rotork Pneumatic Actuator GP series

RWTÜV

Functional Safety Data

Manufacturer Rotork Fluid System S.r.l.
Via del Casalino, 6
I-55012 Tassignano (LU)
Product Pneumatic Actuator
Model / Series GP
Application designed to be used in a Safety Instrumented System for use in low demand application (Emergency Shut Down / Emergency Blow Down)

Reference Report RWTÜV Assessment Report No. 278J06001/A

FUNCTIONAL SAFETY DATA

Reference Standard IEC 61508:2000, part 1 to 7
Functional Safety of electrical/electronic/programmable electronic safety related systems

Type A
Hardware Fault Tolerance 0
Mode Low Demand

λ_d [1/h]	λ_s [1/h]	$\lambda_{dd(ps)}$ [1/h]	SFF (Partial Stroke Test)	SFF (No Partial Stroke Test)
$2,17 \cdot 10^{-8}$	$2,17 \cdot 10^{-7}$	$1,62 \cdot 10^{-8}$	97,7 %	90,9 %

$PFD_{AVG} = 3,02 \cdot 10^{-5}$
(for TI (Test Interval) = 1 year; TI_{ps} (Test Interval Partial Stroke) = 1 month)
See RWTÜV Assessment Report No. 278J06001/A for complete tables of results.

As per these values, based on RWTÜV Assessment Report No. 278J06001/A in the valid version, the Rotork Pneumatic Actuators Series GP can be used up to SIL 3 as a single device.
A user of the Rotork Pneumatic Actuators Series GP can utilize these failure rates in a probabilistic model of a Safety Instrumented Function (SIF) to determine suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL).

Date 2006-04-26

Carlo Tarantola
Carlo Tarantola

RWTÜV Italia S.r.l.
Via Pisacane, 46 - I-20026 Legnano

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	DWG No	200177AT_SIL_00002
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 26	OF N° 29

7.8 Rona Ball Valve ANSI 900

Certificate no: ROT 0608117
Page 1 of 1



Office: Rotterdam

Date: 21 December 2006

This certificate is issued to Truflo Rona s.a. based on DIAC (Dependable Industrial Automation Consultancy) report. In order to certify that the undersigned Surveyor has carried out a review of the Safety Integrity Level - SIL: Classification performance assessment of the following Truflo Rona s.a. product to comply with IEC 61508:

-SIL-3 Duty Certified Quarter Turn Actuator actuated Truflo Rona Ball Valve Assembly
of material properties Stainless Steel, DUPLEX, Bronze, Carbon Steel, Nickel Alloy and Titanium

The review was based on verifying the compliance with IEC 61508 with regard to the following aspects:

- method used
- consistency throughout the report
- clearness of communication evidence
- justification of evidence & source references

The IEC 61508's first premises is that there is equipment intended to provide a function, there is a system which controls it, and between them they pose a risk.

The standard's second premises is that " safety functions " are to be provided to reduce the risk posed by the " Equipment Under Control " (EUC) and it's control system.

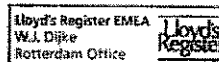
Any system which is designated to implement the required safety functions necessary to achieve a safe state for the EUC and which are intended to achieve the necessary safety integrity for the required safety function are classified as safety related systems.

Safety integrity is defined as the likelihood of a safety related system satisfactorily performing the required safety functions under all stated conditions, within a stated period of time and a safety integrity level (SIL) as a discrete level for specifying the safety integrity requirements of the safety functions.

We hereby confirm that the above is reflected in the DIAC report no. DIAC - TFR - 2006 - 081 - R1, December 2006, as a result of the method applied, demonstrated consistency, desineness of communicated evidence and the justification of evidence and source references.

Results are such that Truflo Rona s.a. SIL-3 Duty Certified Quarter Turn Actuator actuated Ball Valve assembly is confirmed to be capable to perform at SIL - 3 in a single valve configuration and to perform at SIL 4 in a double valve configuration taking into account conservative failure data at a half year Proof Test interval time for both SIL - 3 and SIL - 4

The recommendation as laid down in the DIAC report is to be followed.



Eur. Ing. W.J. Dijk, C.Eng. M.I.Mech.E.
Surveyor to Lloyd's Register EMEA
A member of the Lloyd's Register Group

Lloyd's Register, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as the 'Lloyd's Register Group'. The Lloyd's Register Group assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register Group entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

Form 1124 (2005.02)

A513P

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
SIL ANALYSIS REPORT			DWG NO	200177AT_SIL_00002
			FILE	
This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N° 27	OF N° 29

Table 8: Summary of Applied Failure Rates

Item	Failure Rate Generic [1/hour]	Failure Rate - Dangerous [1/hour]	MTBF-D [ops years]	MFG Multiple Failure Group
Initiator – Pressure Transmitter – Generic Smart – analysis applied	8.33E-6 (ISA/ TP84, Lit. 8)	2.5E-6 (80% unsafe failures, 50% DCF)	46	A, D (per 2003 set)
Initiator – Pressure Transmitter – Smart Selected (known closed source)		1.8 E-6	63	
Initiator – Pressure Transmitter – Smart SIL2 Certified – Certificate values (known closed source)	0.73 E-6 SFF= 79% DCF= 40.9%	0.246 E-6	463	
Initiator – Pressure Transmitter – Smart SIL2 Certified		0.57 E-6	200	
SIL3 Certified Solenoid valve – Certificate Values – low demand (known closed source)		PFD= 0.985 E-4 2.25 E-8 [1/h] at Proof test 1 year	5070	
SIL3 Certified Solenoid valve – Certificate Values – high demand (known closed source)		9.838 E-8	1160	
SIL3 Certified Solenoid valve		1.14 E-7	1000	(F)
Generic SIL3 AK5 redundant PLC (source ISA/ TP84, high DCF) DU value (known closed source)		3.0 E-8 DU value	3800 DU value	E
SIL4 Solid State Electric/Electronic Minimum performance level DU value (known closed source)		4.57 E-9 DU value	25000 DU value	(E)
Generic Final Element - Generic Valve inc. actuator, benchmark analysis applied for the generic case	12.4 E-6 (source ISA/ TP84)	3.7 E-6 (80% unsafe; DCF= 50%)	31	B
Applied: generic Solenoid Valves		3.0 E-7	380	F
SIL-3 Duty Certified Quarter Turn Actuator: Rotork GP Actuator is applied as an example		1.14 E-8	5260	G
Truffo Rona Ball Valve		9.1 E-8	1400	B
Assembly SIL-3 Duty Certified Quarter Turn Actuator applying the Rotork GP Actuator and Truffo Rona Ball Valve (MTBF combination of 5260 and 1400 operational years)		1.04 E-7	1100	(V)

Fault Tree Analysis based SIL calculations results are summarised in Table 9.

Results are presented in Figure 9 - Figure 10 to provide overview and summary per analysis as well as detailed calculation references. Note that application of more generic performing initiators (sensors) and solenoid valves limit the SIL achieved as well as limit the length of the proof test interval time. In the analyses presented a half year proof test interval time is taken as basis.

From practical experience with design of high performance SIL-4 HIPPS's a one year proof test interval time is well achievable with the deployment of instrumentation (initiators/ sensors, solenoid valves, logic solvers) with certified high demonstrated performance.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV.
 CCI We Solve Control Valve Problems™ CCI Valve Technology GmbH Lembockgasse 63, A-1230 Wien			DWG No	200177AT_SIL_00002
			FILE	
SIL ANALYSIS REPORT This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request			SHEET N°	28
			OF N°	29

10 CONCLUSIONS

Design Review Truflo Rona Ball Valve

- 10.1 The Truflo Rona Ball Valve is classified as IEC61508 Type A equipment.
- 10.2 The Manual Proof Test Diagnostic Coverage Factor, for all FMECA Events calculated according to the Safe Failure Fraction for Full Stroke on demand is equal to 95.7% considering all failure rates SU, SD, DD and DD are equal; calculation upon the MTBF based Risk values this value is equal to 98.2%.
- 10.3 The Manual Proof Test Diagnostic Coverage Factor, for FMECA Event1 (Full Stroke Failure) calculated according to the Safe Failure Fraction for Full Stroke on demand is equal to 94.3% considering all failure rates SU, SD, DD and DD are equal; calculation upon the MTBF based Risk values this value is equal to 97.2%.
- 10.4 The SFF and DCF are found to be equal and conservatively well greater than 90%, hence the Truflo Rona Ball Valve having no hardware tolerance can be considered for process service duty in a Single Valve at SIL3 according to IEC 61508 Part 2 SIS architectural requirements.

Failure to deliver on demand a Full Stroke

- 10.5 No Full Stroke Failure caused by the Truflo Rona Ball Valve, operating within agreed service conditions, has been reported at User Companies under survey 1996 until/ including 16 November 2006 covering 1400 operational years. Conservatively One Full Stroke Failure for the Truflo Rona Ball Valve is considered over 1400 operational years, MTBF-D Full Stroke Failure = 1400 operational years.

Safety Instrumented System Benchmark Fault Tree Analysis Results

- 10.6 The SIL-3 Duty Certified Quarter Turn Actuator actuated Truflo Rona Ball Valve assembly has a MTBF-D= 1100 [operational years]. For a one year proof test interval the average PFD becomes 4.55E-4, which is less than 50% of the SIL-3 interval (a typical guideline value).
- 10.7 The SIL-3 Duty Certified Quarter Turn Actuator actuated Truflo Rona Ball Valve assembly is confirmed to be capable to perform at SIL-3 in a Single Valve configuration taking into account conservative failure data at a half year Proof Test Interval Time.
- 10.8 The SIL-3 Duty Certified Quarter Turn Actuator actuated Truflo Rona Ball Valve assembly is confirmed to be capable to perform at SIL-4 in a Double Valve configuration taking into account conservative failure data at a half year Proof Test Interval Time.
- 10.9 A SIL-3 Duty Certified quarter turn actuator having a MTBF-D (Full Stroke Failure) of at least 5000 operational years is required (at least once per year a Full Stroke Test). As an example SIL Calculations considered applied the Rotork GP quarter turn Actuator with MTBF-D of 5250 operational years.
- 10.10 Based upon the current status of performance information the Truflo Rona Ball Valve could be capable to perform at a one year proof test interval time at Single Valve SIL-3/ Double Valve SIL-4 configuration in a sound engineered Safety Instrumented System design where due consideration is given to matching the instrumentation to the actual process conditions and where the potential for development of time-based valve errors are operationally considered and reflected in appropriate proof test interval times.

11 RECOMMENDATIONS

- 11.1 Considering the conservative approach it is recommended to review the safety-related performance again after approximately three years.

B	05_09_2007	ADDED ABBREVIATIONS AND FAILURE RATES (sh: 2, 11, 23)	Fusi L.	Pucci P.
A	26_07_2007	FIRST ISSUE	Fusi L.	Pucci P.
REV.	DATE	DESCRIPTION	PREPARED	CHECK/APPROV
 We Solve Control Valve Problems® CCI Valve Technology GmbH Lemböckgasse 63, A-1230 Wien		SIL ANALYSIS REPORT	NO	200177AT_SIL_00002
			DWG No	
			FILE	
			This document is property of CCI Valve Technology GmbH. It is strictly confidential and must not be copied, traced or loaned without their written permission and has to be returned upon request	
			SHEET N° 29	OF N° 29

V&C C KPC-2417 (code-A)